www.huawei.com

© 2018

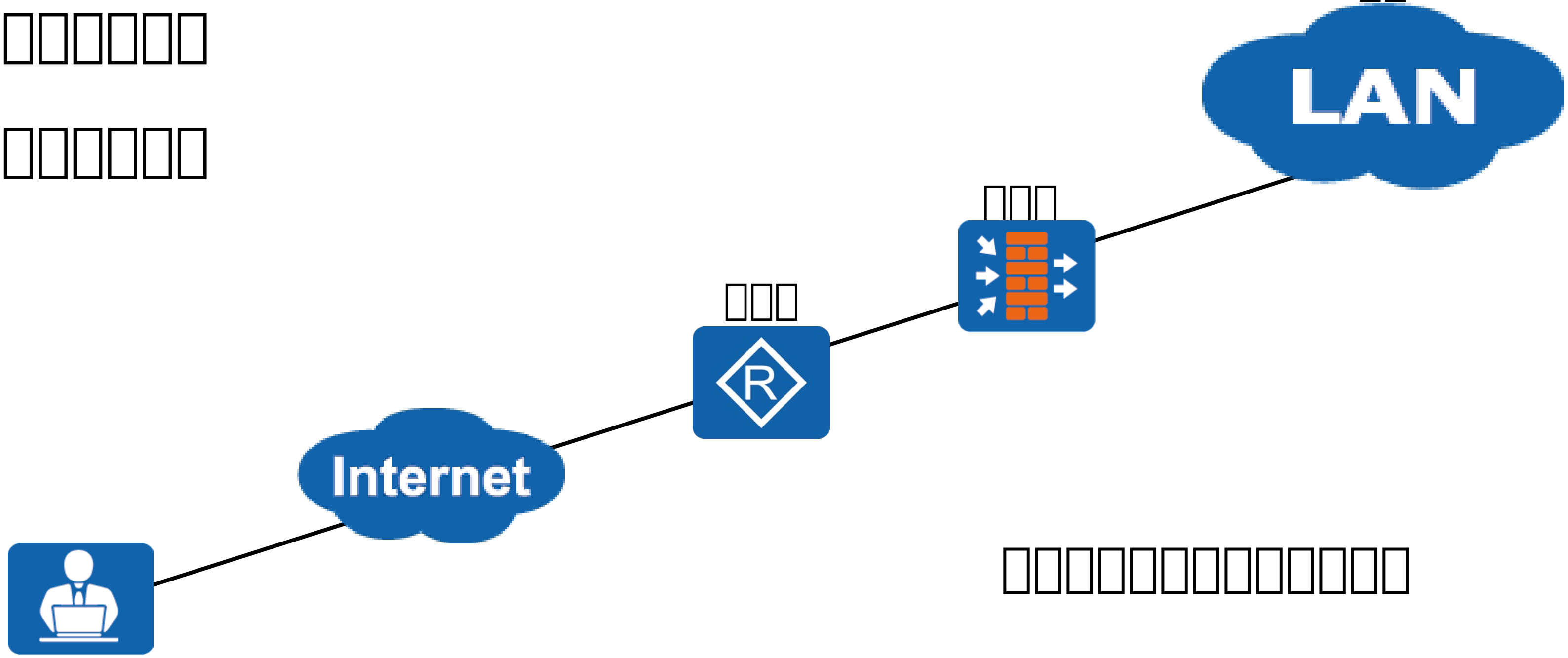
[illegible]

- [illegible]
- [illegible]

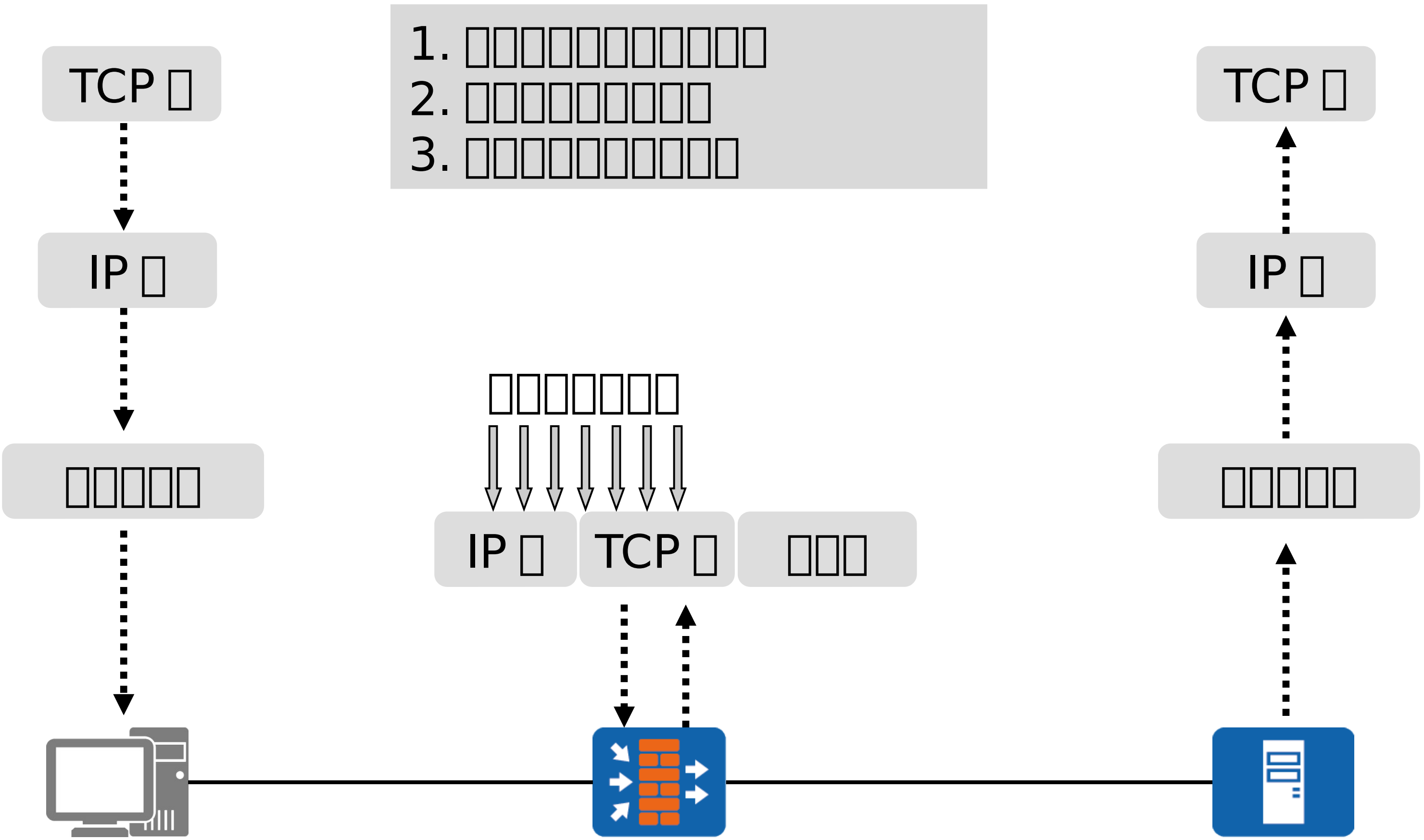
[illegible] © 2018 [illegible]

[illegible]

1. [illegible]
2. [illegible]
3. [illegible]
4. ASPF [illegible]

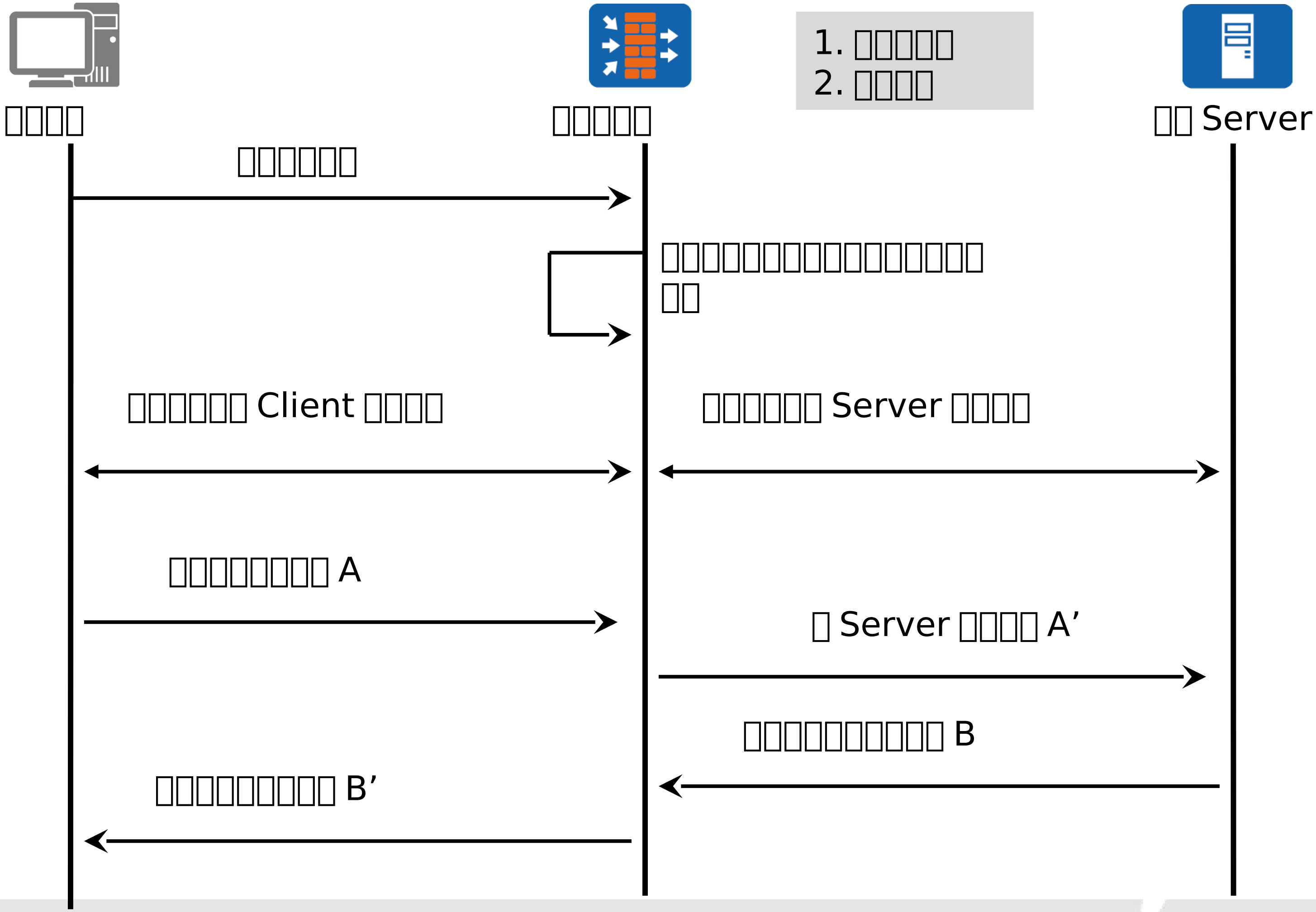

LAN
R
Internet

[illegible] - [illegible]



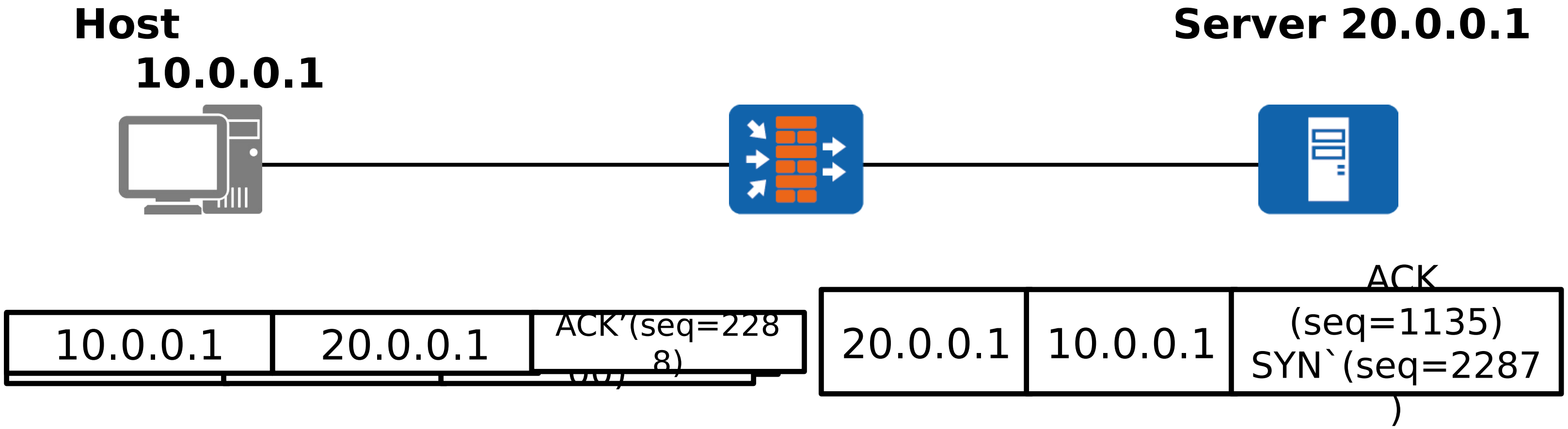
[illegible] © 2018 [illegible]

□□□□□ - □□□□□



1. □□□□□
2. □□□□
□□□□
□□□□□
□□ Server
□□□□□□
□□□□□□□□□□□□□□□□□
□□
□□□□□□ Client □□□□
□□□□□□ Server □□□□
□□□□□□□□ A
□ Server □□□□ A’
□□□□□□□□□□ B
□□□□□□□□□ B’

[illegible] - [illegible]



Host
10.0.0.1
Server 20.0.0.1
10.0.0.1
20.0.0.1
ACK’(seq=228
8)
20.0.0.1
10.0.0.1
ACK
(seq=1135)
SYN`(seq=2287
)

[illegible]

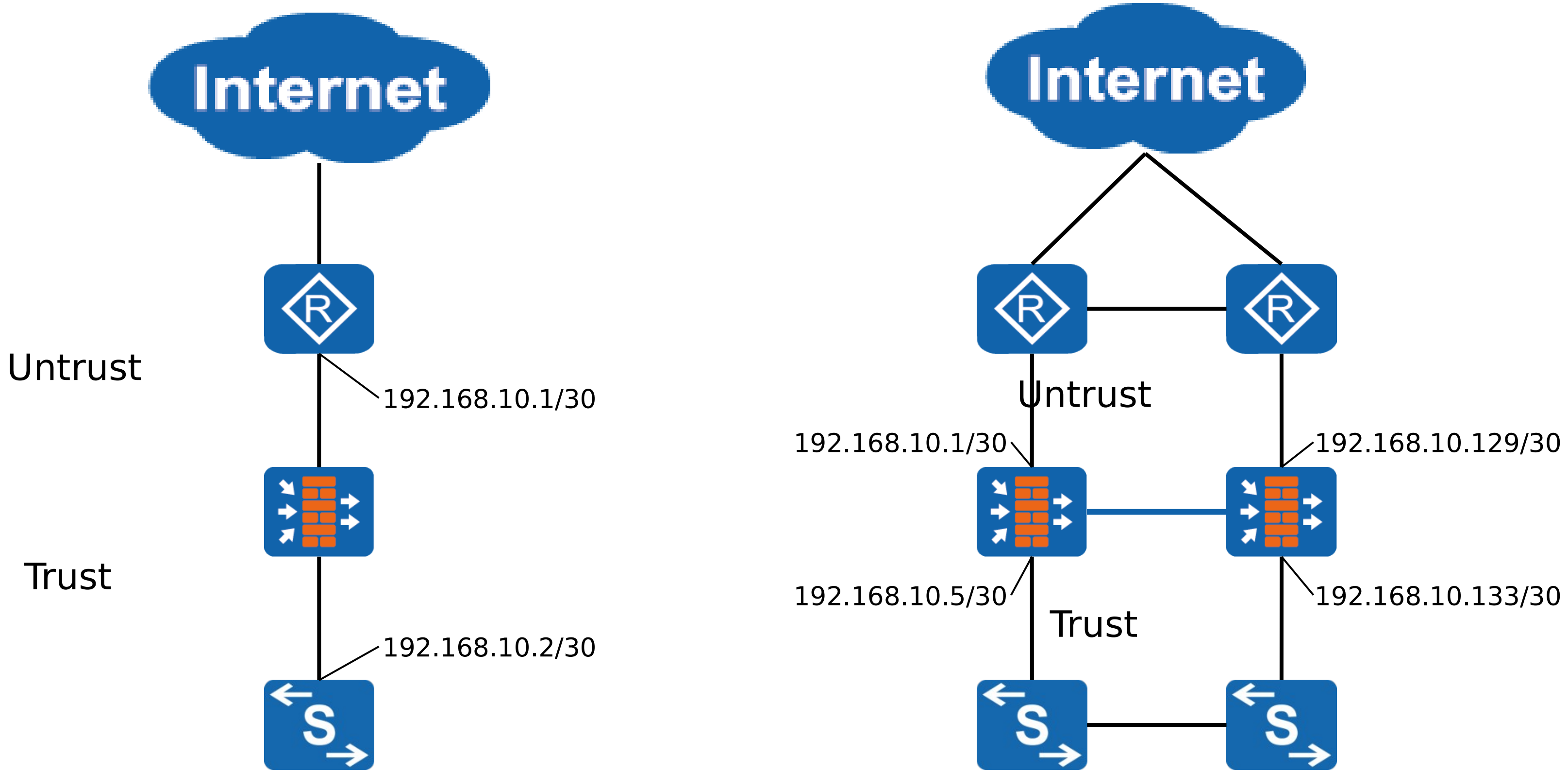
[illegible]

[illegible]

1. [illegible]
2. [illegible]

[illegible] © 2018 [illegible]

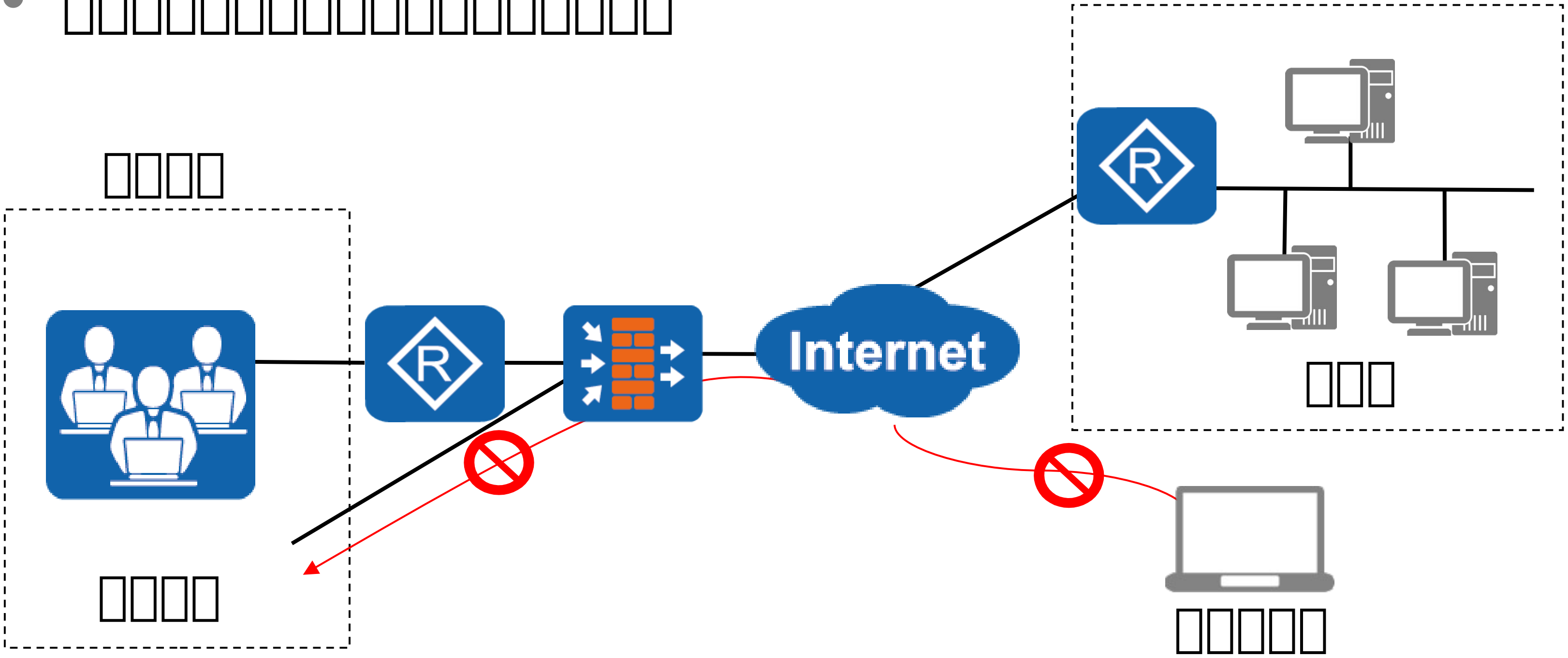
[illegible]


Internet
Untrust
192.168.10.1/30
Trust
192.168.10.2/30
Internet
Untrust
192.168.10.1/30
192.168.10.129/30
192.168.10.5/30
192.168.10.133/30
Trust

[illegible]

1. [illegible]
2. **[illegible]**
3. [illegible]
4. ASPF [illegible]

[illegible] © 2018 [illegible]


Internet

[illegible]

[illegible]

Policy 0 [illegible] A [illegible]

Policy 1 [illegible] B [illegible]

[illegible]

[illegible] 2 [illegible]

[illegible]

[illegible]

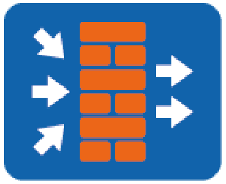
[illegible]

[illegible]

[illegible] 1 [illegible]

[illegible]

BBAABBBAAAA



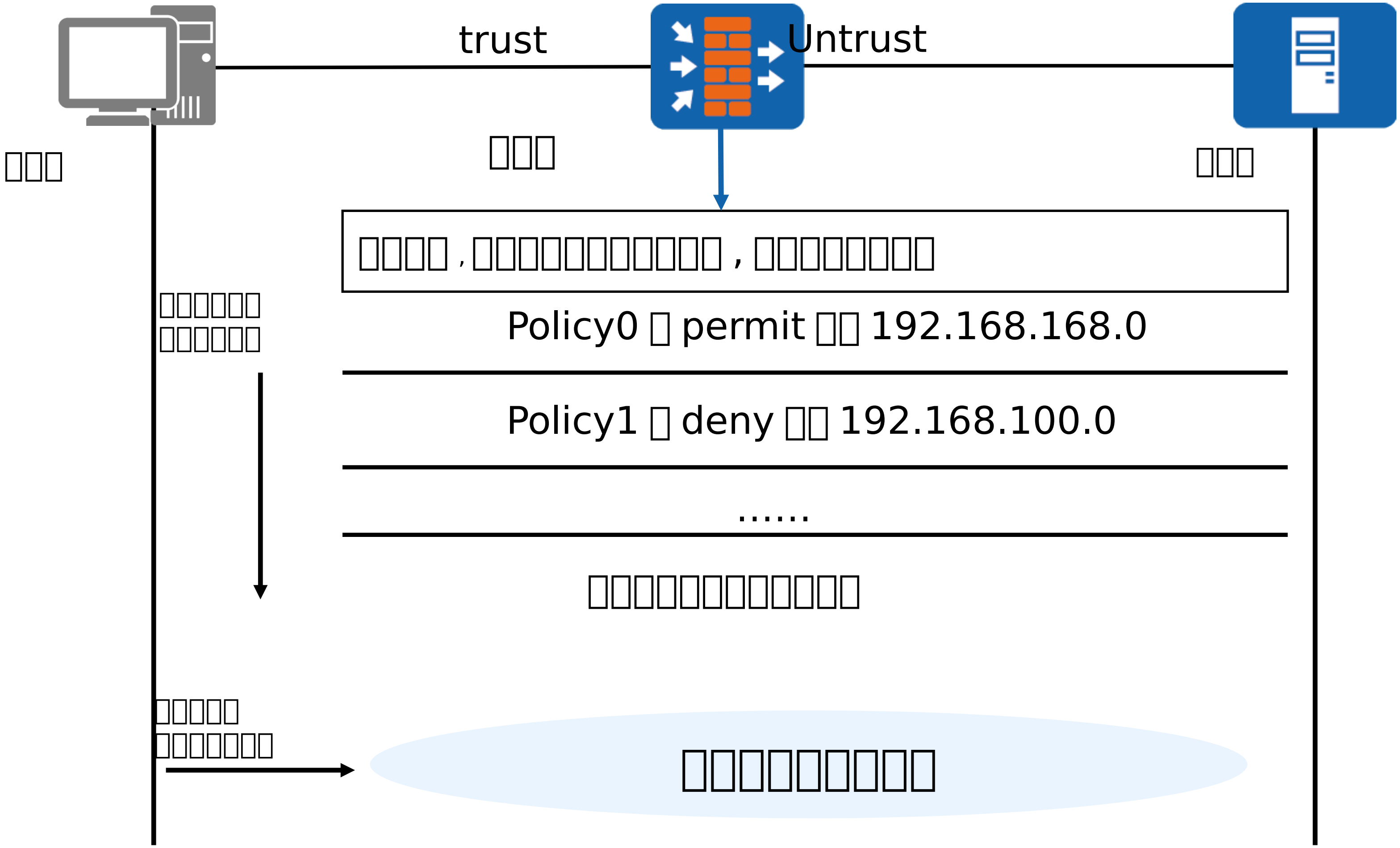
AA AAAA

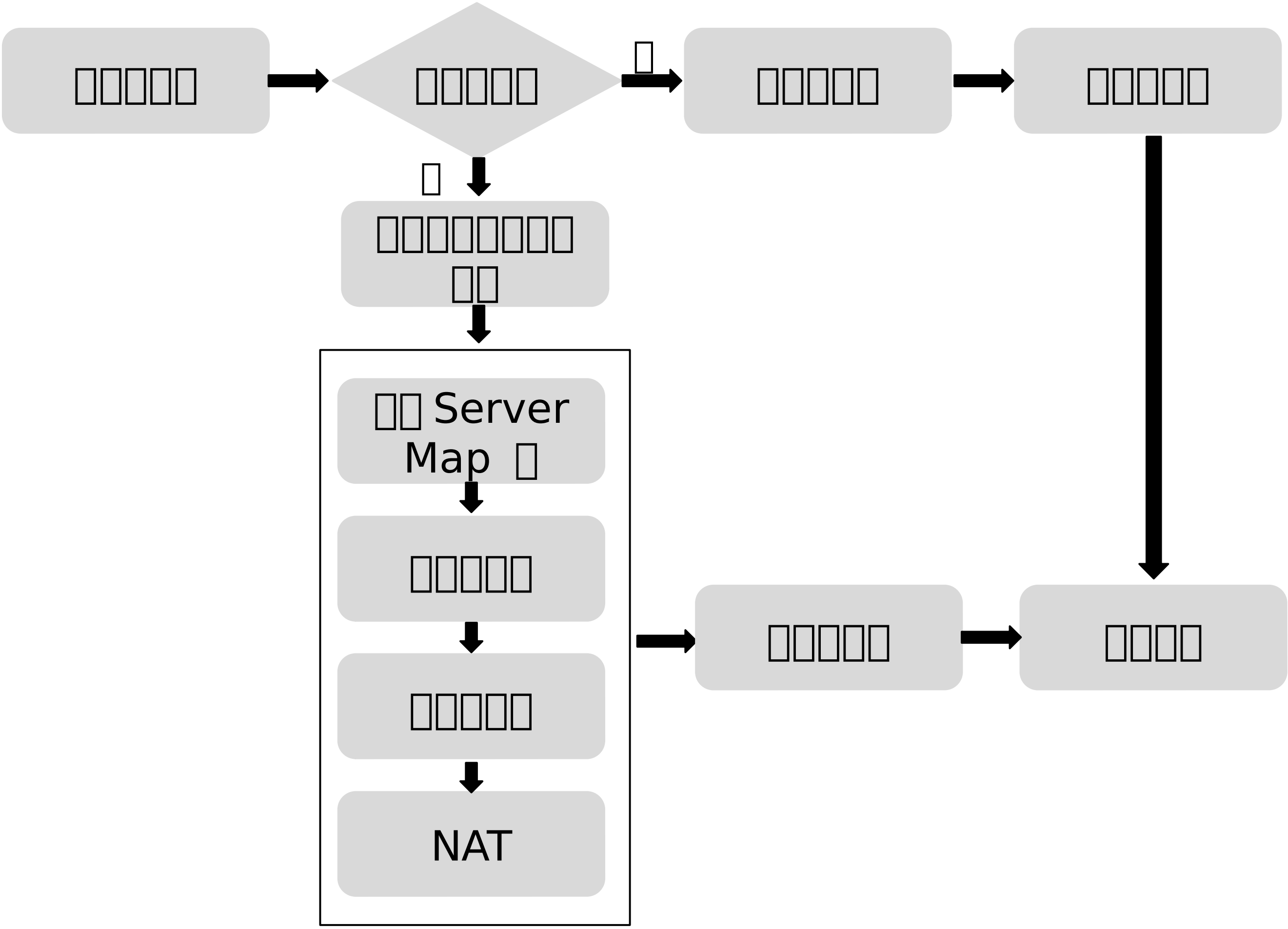
[illegible]

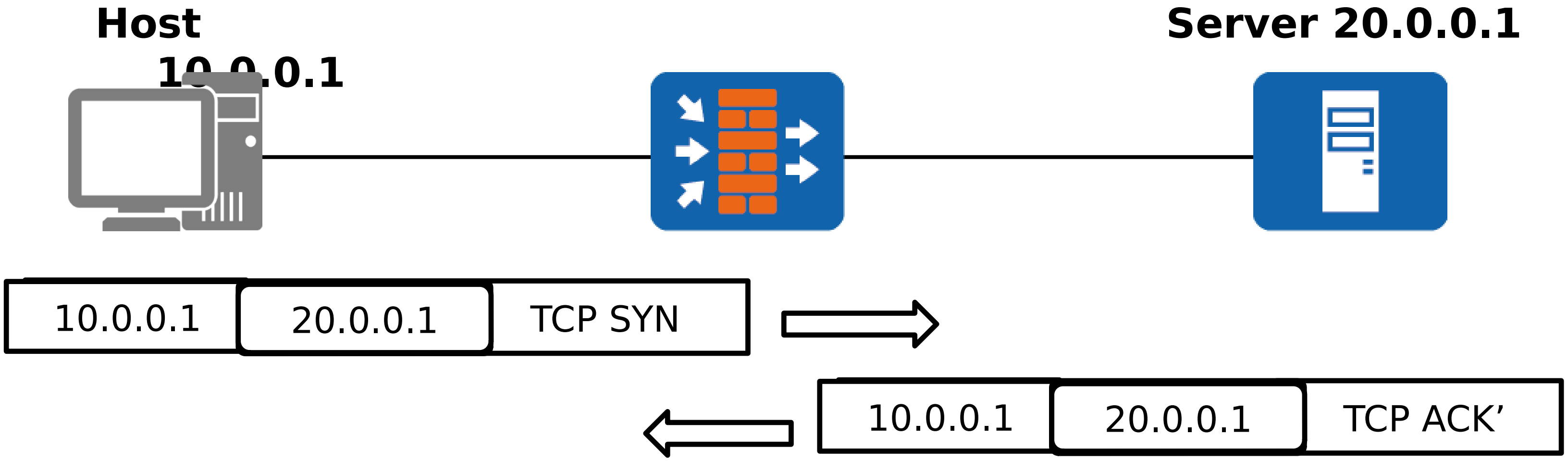
[illegible]

- [illegible]

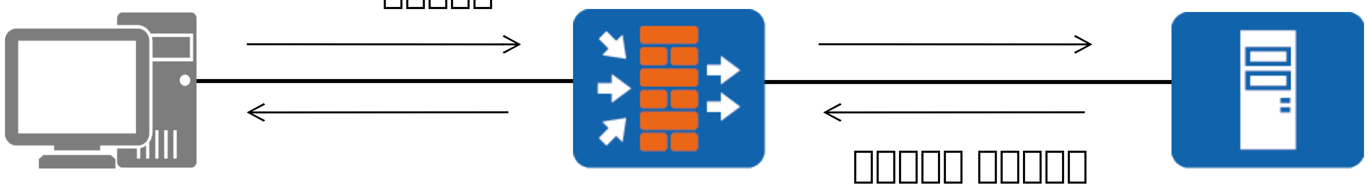
  [illegible]


trust
Untrust
Policy0 permit 192.168.168.0
Policy1 deny 192.168.100.0
......


Server
Map
NAT


Host
10.0.0.1
Server 20.0.0.1
10.0.0.1
20.0.0.1
TCP SYN
10.0.0.1
20.0.0.1
TCP ACK’

□□□□



Client□ Server

□ IP □□	□□□	□□ IP □□	□□□□	□□	□□	□□
192.168.1.1	20000	1.1.1.1	23	TCP	abc	Telnet

Server□ Client

□ IP □□	□□□	□□ IP □□	□□□□	□□	□□	□□
1.1.1.1	23	192.168.1.1	20000	TCP	abc	Telnet

Session: TCP 192.168.1.1:20000 □ 1.1.1.1:23

□□□□□□□

- □□□□□□□□□ display firewall session table

```
<sysname> display firewall session table
Current Total Sessions : 2
   telnet VPN:public --> public 192.168.3.1:2855-->192.168.3.2:23
   http VPN:public --> public 192.168.3.8:2559-->192.168.3.200:80
```

- □□□□□□□□□ display firewall session table verbose

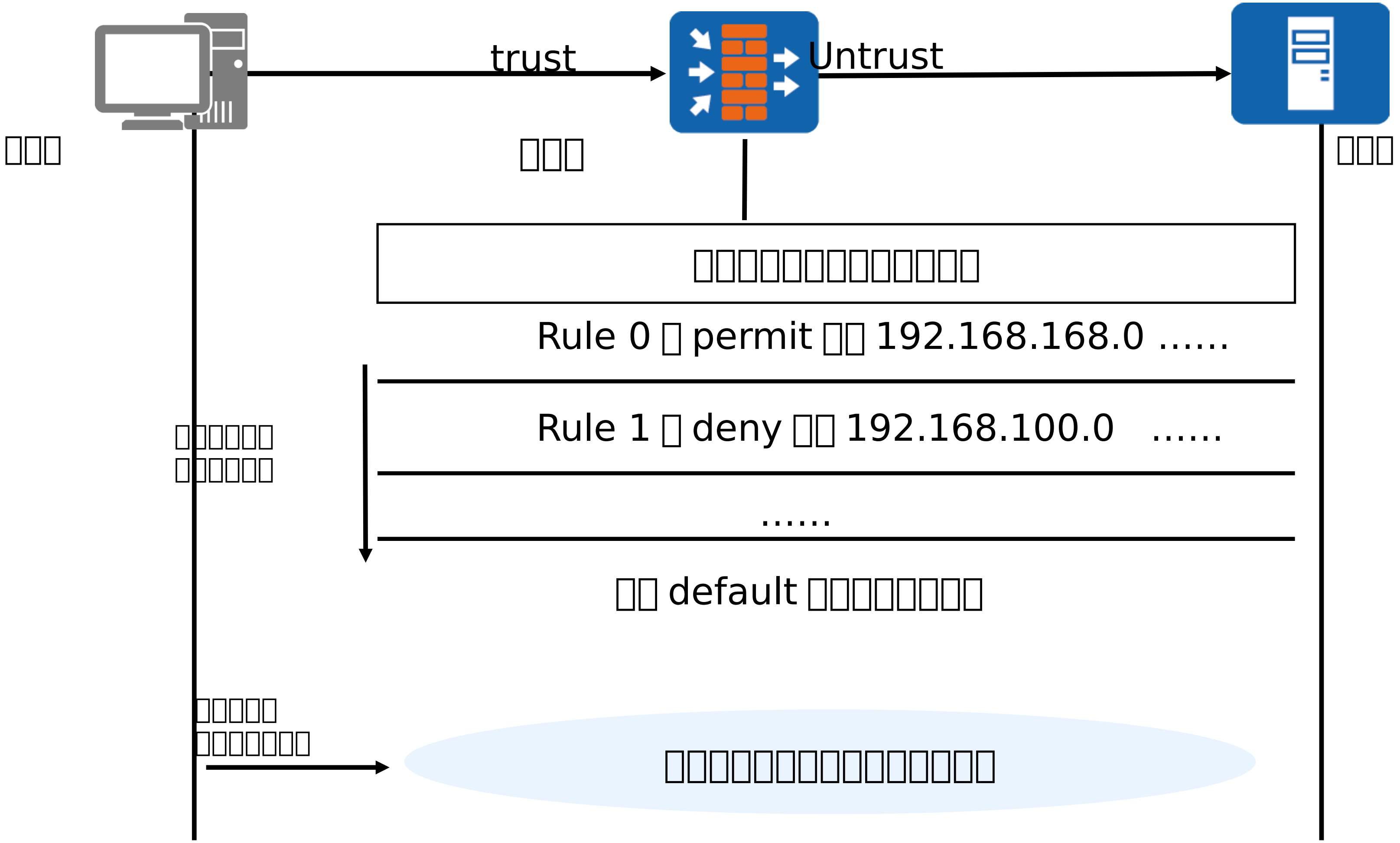
```
<sysname> display firewall session table verbose
Current Total Sessions : 1
   http VPN:public --> public ID: a48f3648905d02c0553591da1
   Zone: trust--> local TTL: 00:20:00 Left: 00:19:56
   Output-interface: InLoopBack0 NextHop: 127.0.0.1 MAC: 00-00-00-
00-00-00
   <--packets:3073 bytes:3251431 -->packets:2881 bytes:705651
   128.18.196.4:1864-->128.18.196.251:80 PolicyName: test
```

□□□□ © 2018 □□□□□□□□

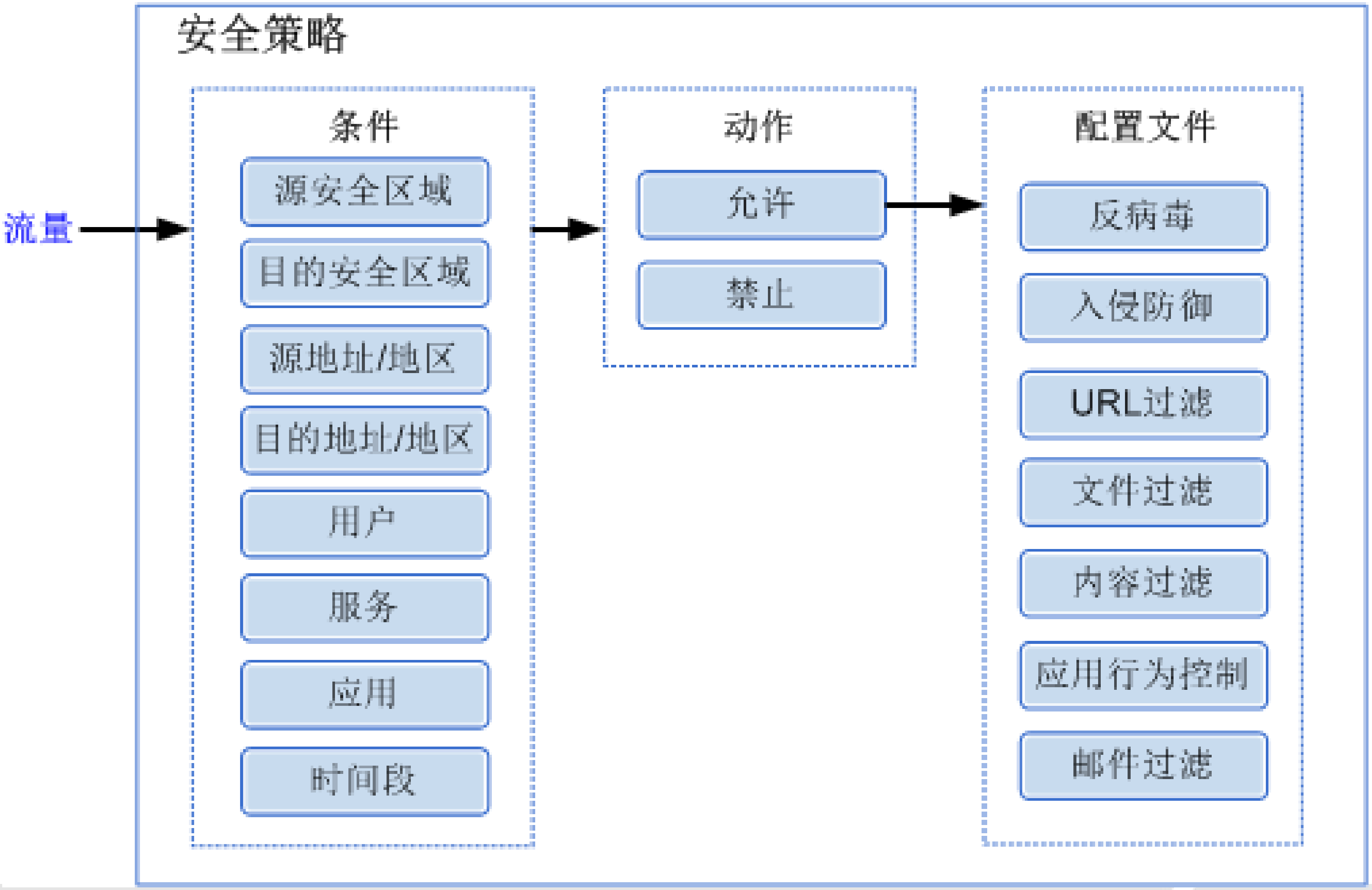
[illegible]

1. [illegible]
2. [illegible]
3. **[illegible]**
4. ASPF [illegible]

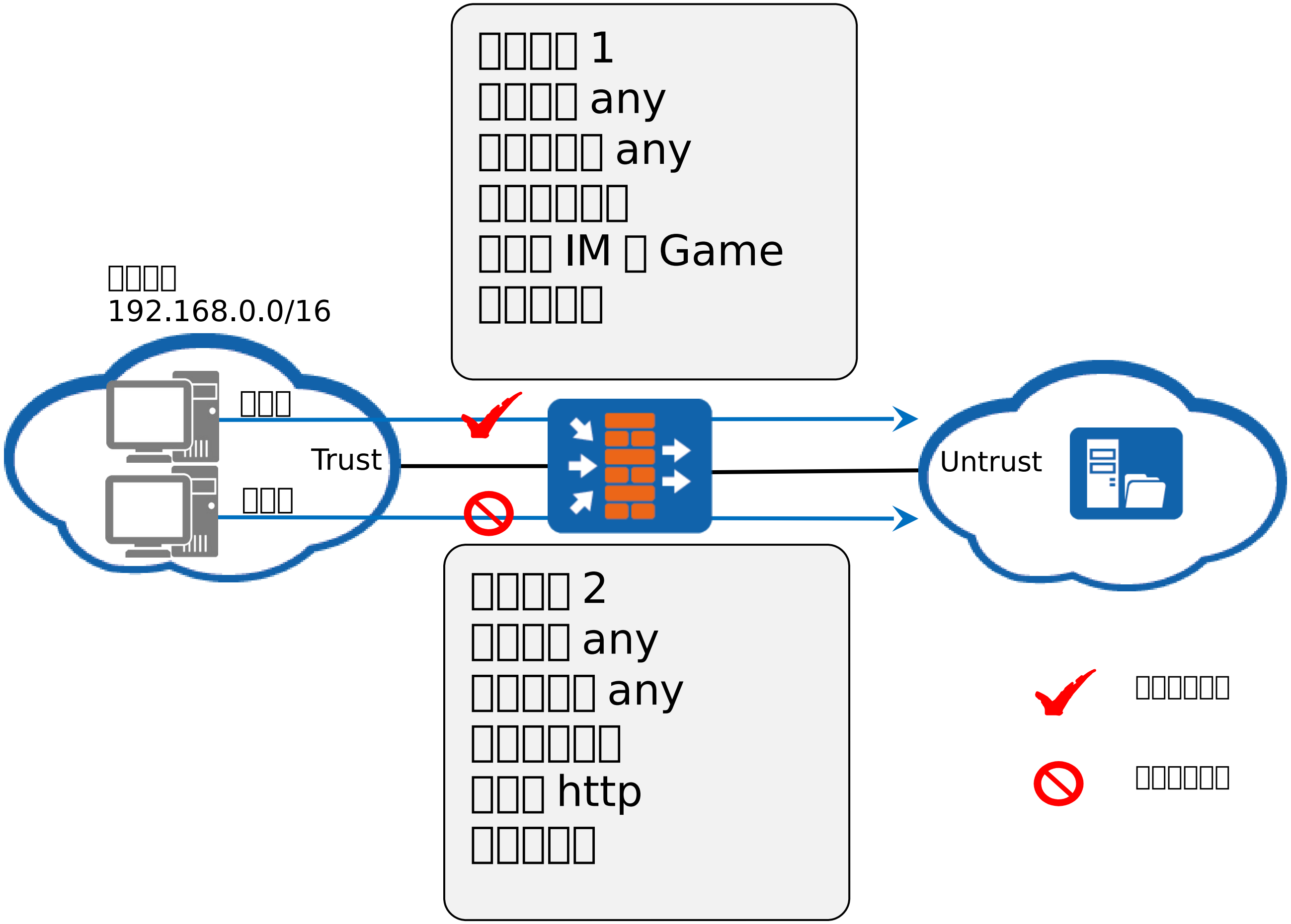
□□□□□□□□□



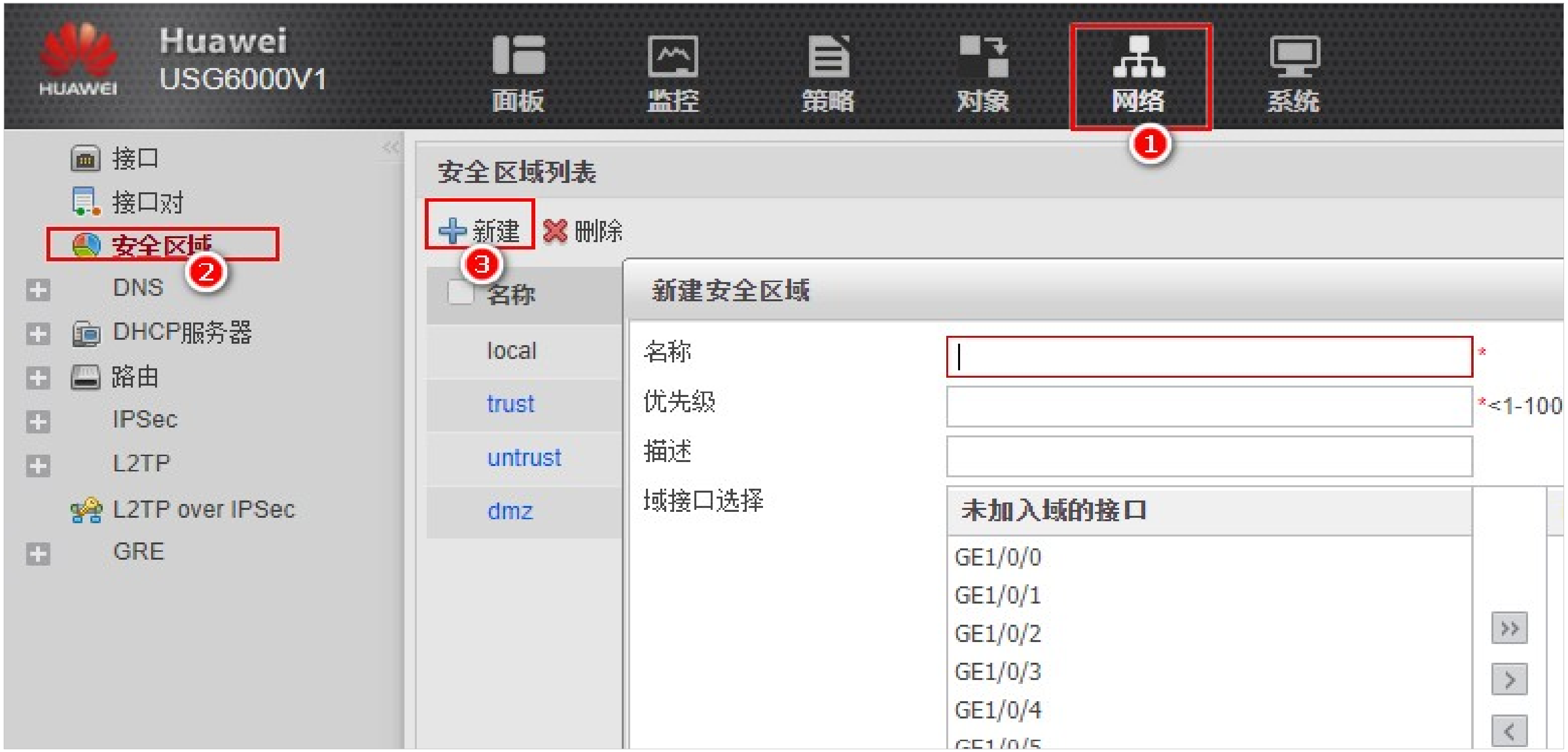
trust
Untrust
□□□
□□□
□□□
□□□□□□□□□□□□□□
Rule 0 □ permit □□ 192.168.168.0 ……
Rule 1 □ deny □□ 192.168.100.0 ……
……
□□□□□□
□□□□□□
□□ default □□□□□□□□
□□□□□
□□□□□□□
□□□□□□□□□□□□□□□


安全策略
流量
条件
源安全区域
目的安全区域
源地址/地区
目的地址/地区
用户
服务
应用
时间段
动作
允许
禁止
配置文件
反病毒
入侵防御
URL过滤
文件过滤
内容过滤
应用行为控制
邮件过滤

□□□□□□


□□□□ 1
□□□□ any
□□□□□ any
□□□□□□
□□□ IM □ Game
□□□□□
□□□□
192.168.0.0/16
□□□
Trust
□□□
Untrust
□□□□ 2
□□□□ any
□□□□□ any
□□□□□□
□□□ http
□□□□□
□□□□□□
□□□□□□

(WEB)



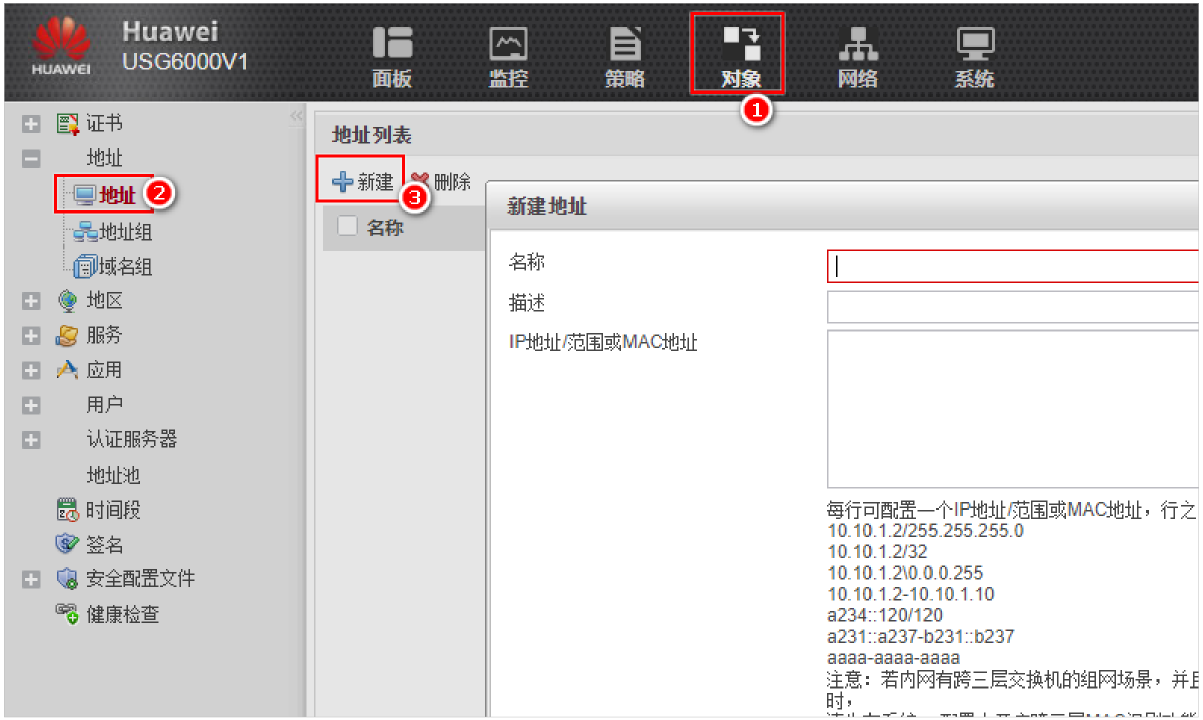
Huawei
USG6000V1
HUAWEI
面板
监控
策略
对象
网络
系统
1
接口
接口对
安全区域
2
DNS
DHCP服务器
路由
IPSec
L2TP
L2TP over IPSec
GRE
安全区域列表
新建
删除
3
名称
local
trust
untrust
dmz
新建安全区域
名称
*
优先级
*<1-100
描述
域接口选择
未加入域的接口
GE1/0/0
GE1/0/1
GE1/0/2
GE1/0/3
GE1/0/4

[illegible] (WEB)

- [illegible]:
  - [illegible]
  - [illegible]
  - [illegible] Profile [illegible] URL [illegible]

[illegible] (WEB)

- [illegible] IPv4/IPv6 [illegible] MAC [illegible]
- [illegible] IPv4/IPv6 [illegible] MAC [illegible] NAT [illegible]



[illegible]（WEB)

- [illegible] IP [illegible] IP [illegible]
- [illegible]

Huawei
USG6000V1
HUAWEI
面板
监控
策略
对象
网络
系统
证书
地址
地区
地区
地区组
服务
应用
用户
认证服务器
地址池
时间段
签名
安全配置文件
健康检查
地区
新建
删除
名称
未知区域
中国
北京
上海
天津
重庆
香港
澳门
河北
石家庄
新建地区
名称
描述
经度
纬度
IP地址
0.00
0.00
<-180.00
<-90.00~

□□□□□□□□（WEB)

- □□□□□□□□□□□□□□□□□□□□□□□□□
- □□□□□□□□□□□□□□□□□□□
- □□□□□□□□□□□TCP□UDP□ICMP□□□□□□□□□□□□□□

[illegible]（WEB）

- [illegible]

Huawei
USG6000V1
HUAWEI
面板
监控
策略
对象
网络
系统
当前用户：admin
证书
本地证书
CA证书
CRL证书
证书过滤
地址
地区
服务
应用
应用
应用组
用户
认证服务器
地址池
时间段
签名
安全配置文件
健康检查
应用
新建
删除
复制
导入
导出
刷新
只显示自定义应用
请输入名称
类别
子类别
标签
数据传输方式
通用类应用
网络应用
传统互联网
娱乐
商业系统
IP协议
电子商务
隧道协议
搜索引擎
即时通信文件传输
数据库
企业应用
加密通信
基于P2P的
基于HTTP的
未指定的
服务器-客户端
浏览器
网络
端到端
自定义应用变更之后，需要提交后才能生效。
名称
类别
子类别
标签
数据传输方式
BT
传统互联网
P2P文件共享
造成工作效率下降
造成数据泄露
具有躲避特征
隧道协议
端到端
PPLive网络电视
娱乐
P2P网络视频
可被利用
造成工作效率下降
造成数据泄露
消耗网络带宽
具有躲避特征
隧道协议
端到端
1
2
3

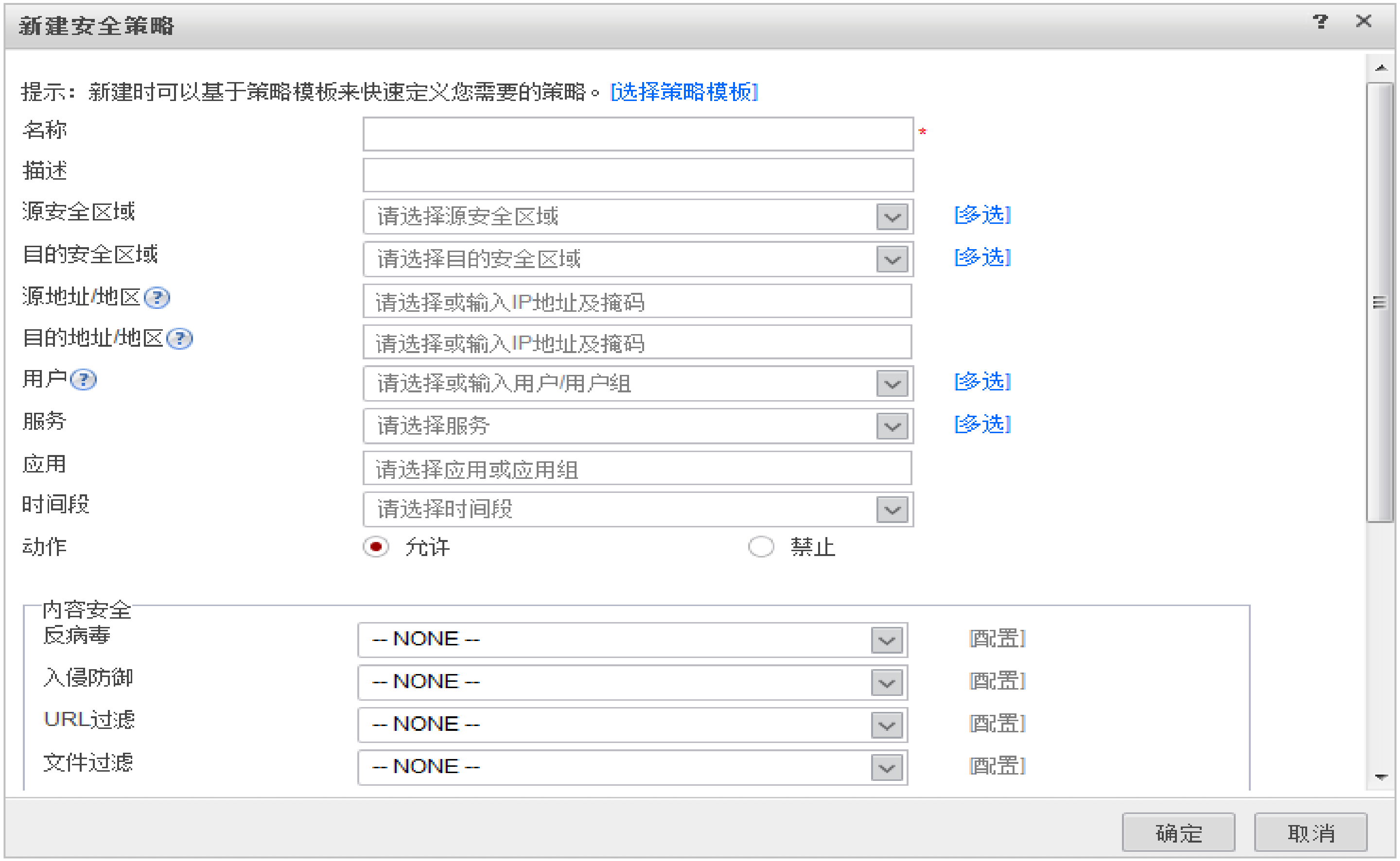
[illegible] (WEB)

- [illegible] NGFW [illegible]

Huawei
USG6000V1
面板
监控
策略
对象
网络
系统
证书
本地证书
CA证书
CRL证书
证书过滤
地址
地区
服务
应用
用户
认证服务器
地址池
时间段
安全配置文件
时间段列表
新建
删除
名称
成员（开始时间 - 结束时间 每周生效时间）
worktime
08:00:00 - 18:00:00 工作日

[illegible]（WEB)

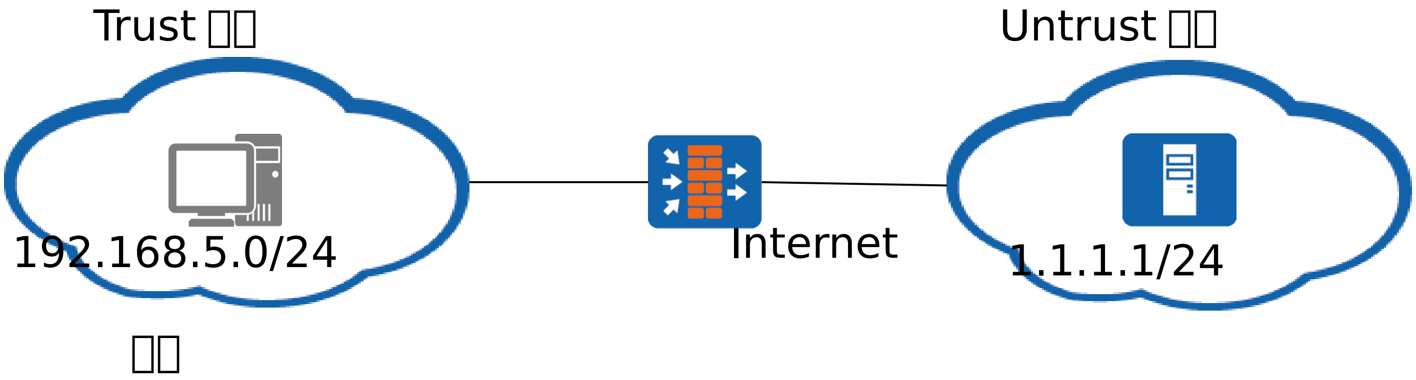
- [illegible]



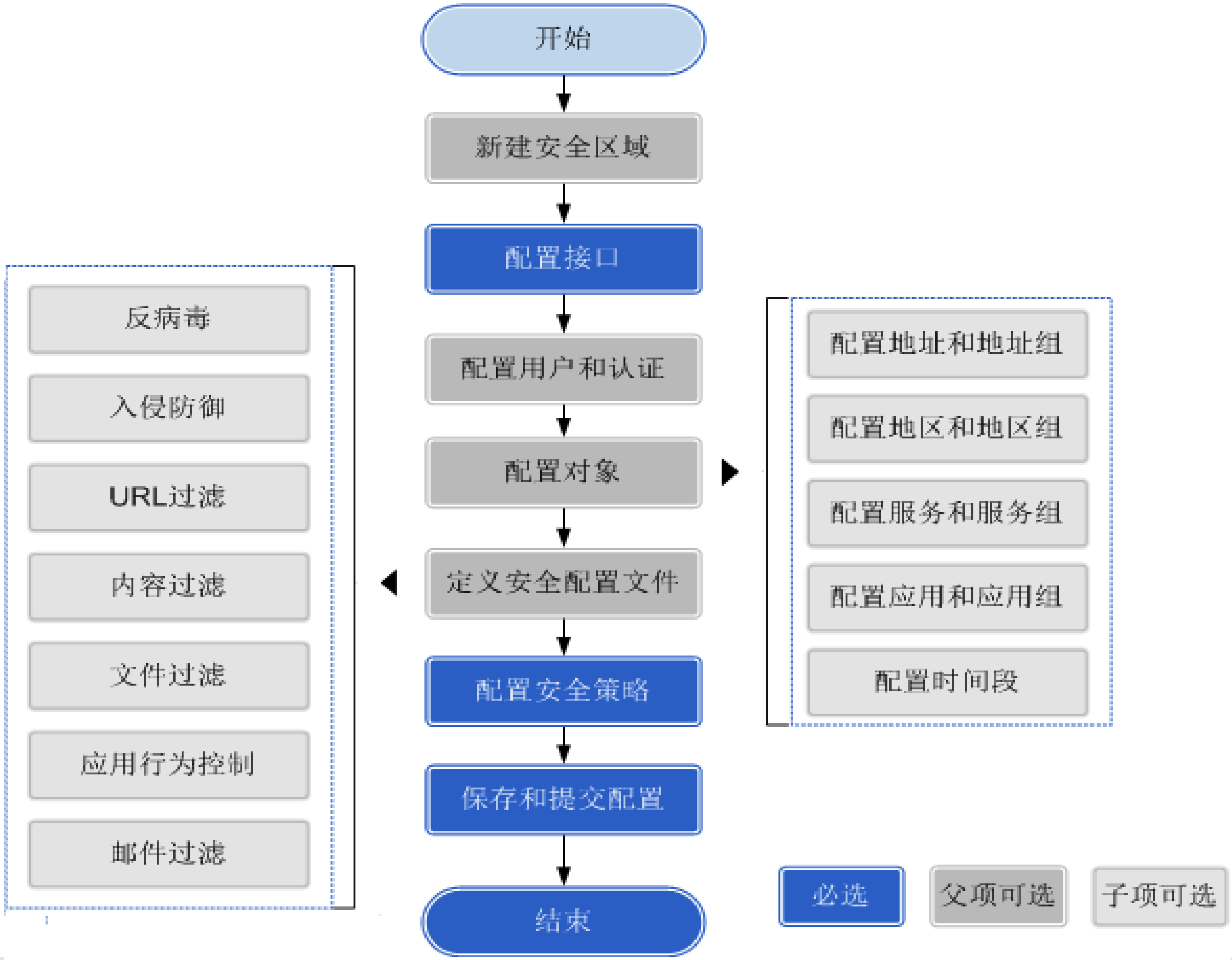
新建安全策略
提示：新建时可以基于策略模板来快速定义您需要的策略。[选择策略模板]
名称
描述
源安全区域
请选择源安全区域
[多选]
目的安全区域
请选择目的安全区域
[多选]
源地址/地区
请选择或输入IP地址及掩码
目的地址/地区
请选择或输入IP地址及掩码
用户
请选择或输入用户/用户组
[多选]
服务
请选择服务
[多选]
应用
请选择应用或应用组
时间段
请选择时间段
动作
允许
禁止
内容安全
反病毒
-- NONE --
[配置]
入侵防御
-- NONE --
[配置]
URL过滤
-- NONE --
[配置]
文件过滤
-- NONE --
[配置]
确定
取消

[illegible]

- [illegible]
  - [illegible] 192.168.5.0/24 [illegible] Internet [illegible] 192.168.5.2 [illegible] 192.168.5.3 [illegible] 192.168.5.6 [illegible] PC [illegible]



□□□□□□□□



开始
新建安全区域
配置接口
配置用户和认证
配置对象
定义安全配置文件
配置安全策略
保存和提交配置
结束
反病毒
入侵防御
URL过滤
内容过滤
文件过滤
应用行为控制
邮件过滤
配置地址和地址组
配置地区和地区组
配置服务和服务组
配置应用和应用组
配置时间段
必选
父项可选
子项可选

□□□□ © 2018 □□□□□□□□

□□□□（□□□）

- □□□□□□□□□□IP□□□□Internet□□□□□□□□□

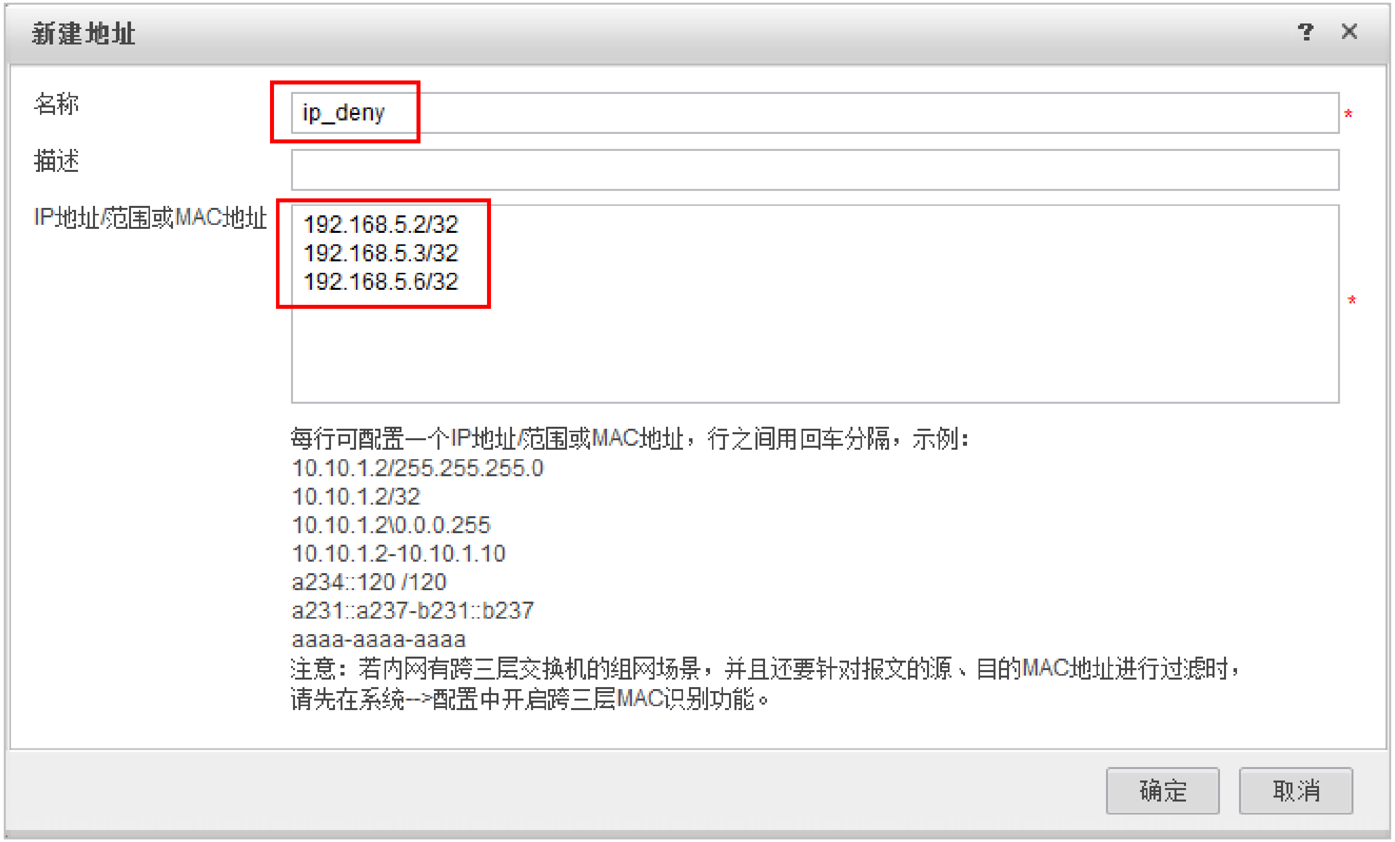
```
[NGFW]security-policy
[NGFW-policy-security]rule name celue
[NGFW-policy-security-rule-celue]source-zone trust
[NGFW-policy-security-rule-celue]destination-zone untrust
[NGFW-policy-security-rule-celue]source-address 192.168.5.2 32
[NGFW-policy-security-rule-celue]source-address 192.168.5.3 32
[NGFW-policy-security-rule-celue]source-address 192.168.5.6 32
[NGFW-policy-security-rule-celue]action deny
```

```
[NGFW]security-policy
[NGFW-policy-security]rule name celue2
[NGFW-policy-security-rule-celue2]source-zone trust
[NGFW-policy-security-rule-celue2]destination-zone untrust
[NGFW-policy-security-rule-celue2]source-address 192.168.5.0 24
[NGFW-policy-security-rule-celue2]action permit
```

□□□□ © 2018 □□□□□□□

□□□□（WEB）- (1)

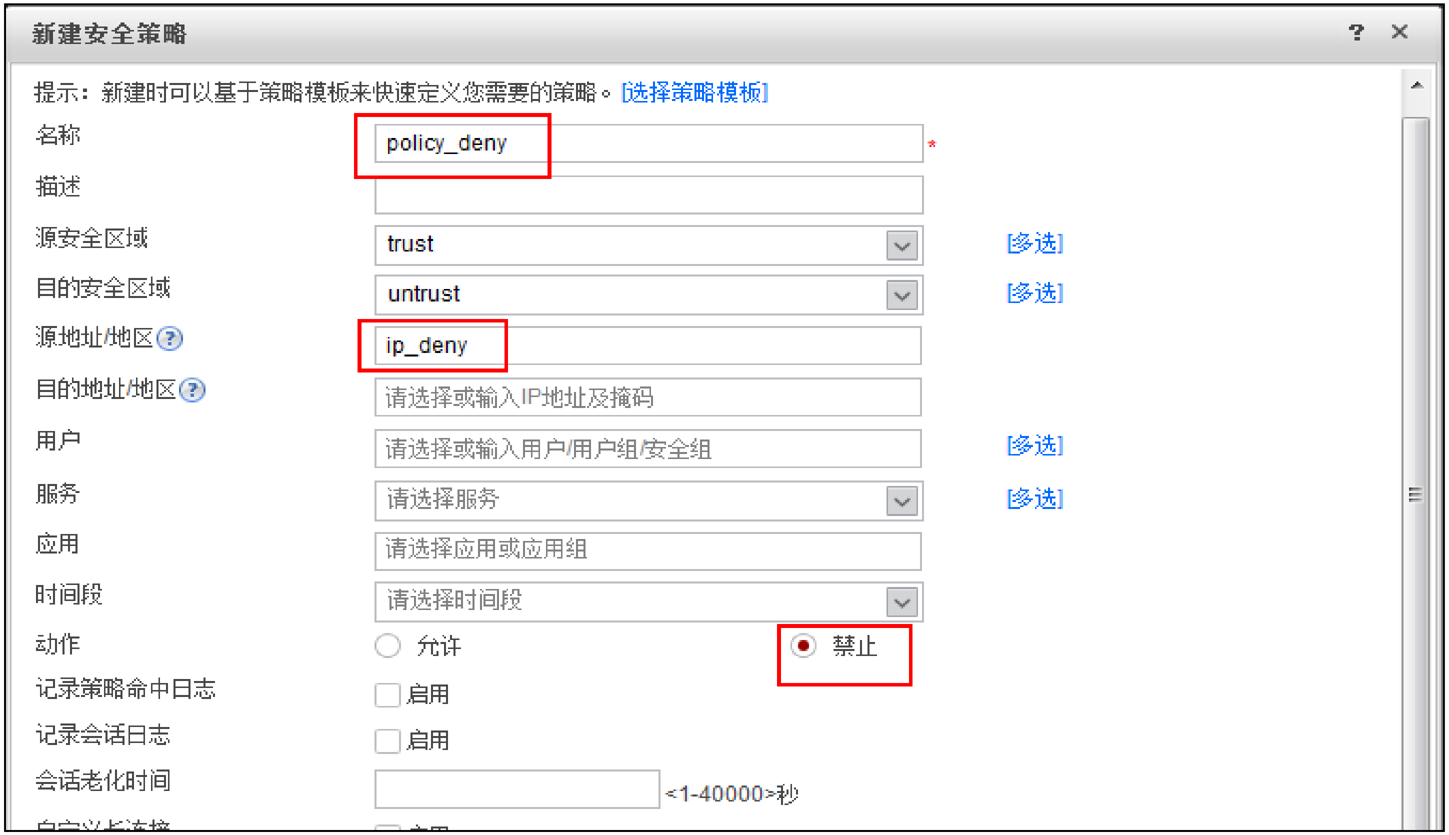
- □□□□□ ip_deny □□□□□



□□□□ © 2018 □□□□□□□

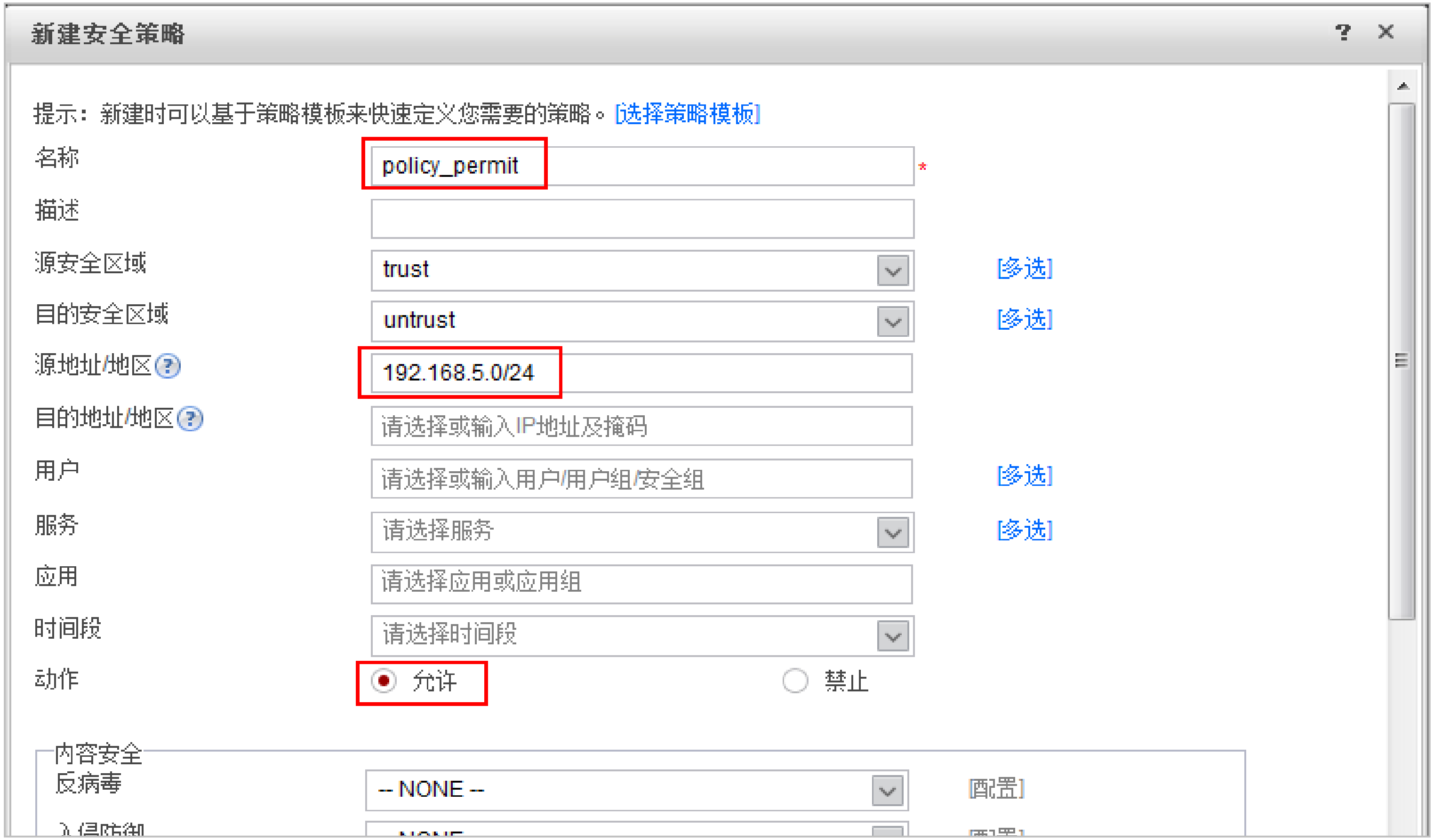
□□□□（WEB) - (2)

- □□□□□□□□□ ip_deny □ IP □□□□ Internet □□□□□□



□□□□（WEB）- (3)

- □□□□ 192.168.5.0/24 □□□□ Internet □□□□□□



[illegible]

1. [illegible]
2. [illegible]
3. [illegible]
4. **ASPF [illegible]**

[illegible] © 2018 [illegible]

[illegible]

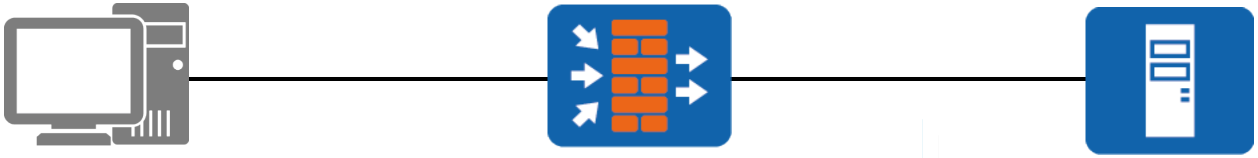
- [illegible] WWW [illegible] 80 [illegible]
- [illegible] FTP [illegible] 21 [illegible]

[illegible]

[illegible]

ASPF [illegible]

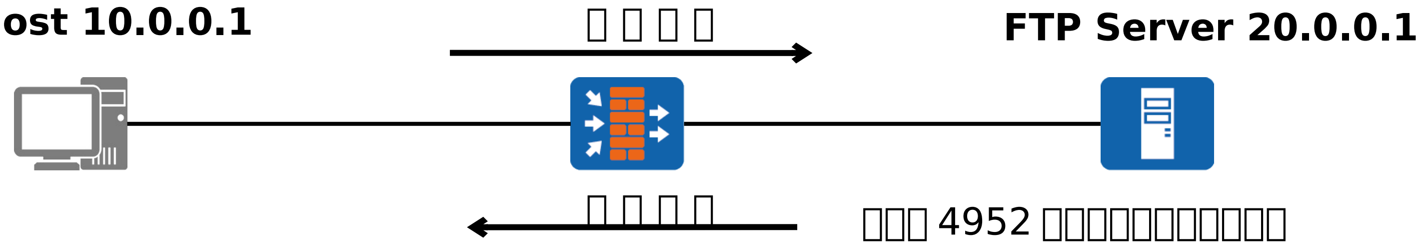
- ASPF (Application Specific Packet Filter) [illegible] [illegible] ASPF [illegible]



[illegible] [illegible]

ASPF □□□□□□□□□□□

- ASPF □ Application Specific Packet Filter □□□□□□□□□□□□□□□




```
Session□        FTP:10.0.0.1:4927 --> 20.0.0.1:21
                 FTP:10.0.0.1:4926 --> 20.0.0.1:4952
```

```
ServerMap  □
------------------------------------------------------------
Inside-Address :Port  Global-Address :Port  Pro   AppType  TTL  Left
------------------------------------------------------------   20.0.0.1
   :  4952     ---
tcp    FTP   DATA     00:01:00  00:00:47
```

□□□□ © 2018 □□□□□□□□

Server Map □□□

□□ ASPF □□□□ FTP □ RTSP □□□□□
□□□□□ Server-map □□□

□□ ASPF □□□□ QQ/
MSN □ TFTP □ STUN □□□□□
□□□□□□ Server-map □□□

Server Map □□□

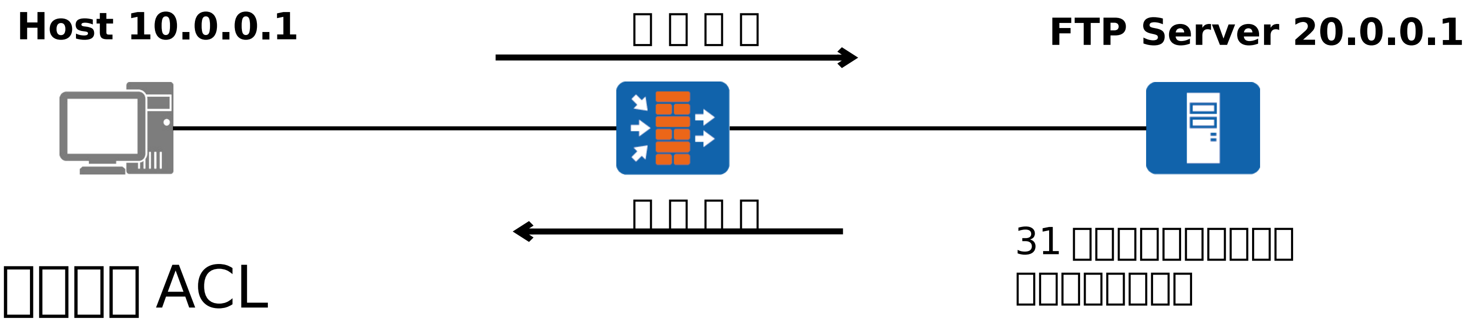
□□ NAT □□□□□□□□□□□□
Server-map □

□□ NAT No-PAT □□□□□□
Server-map □

□□□□ © 2018 □□□□□□□□

□□□□□□□□□□□□□

- □□□□□□□□□□□□□□□□□□



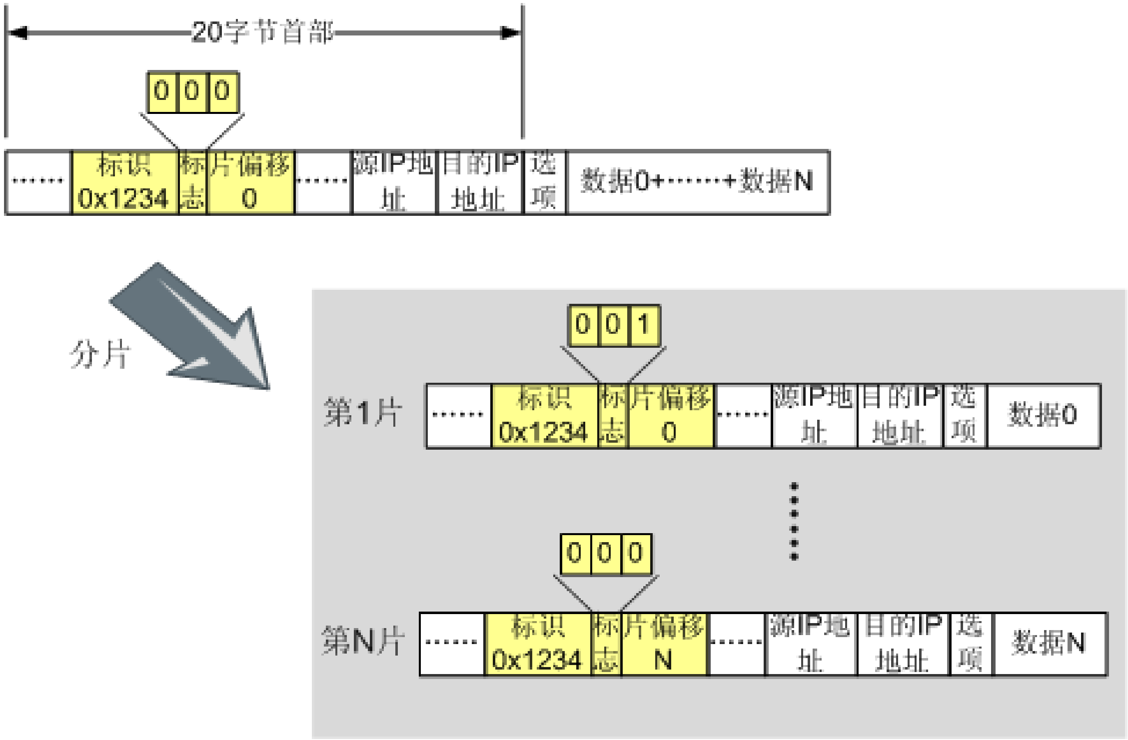
- □□□□ ACL

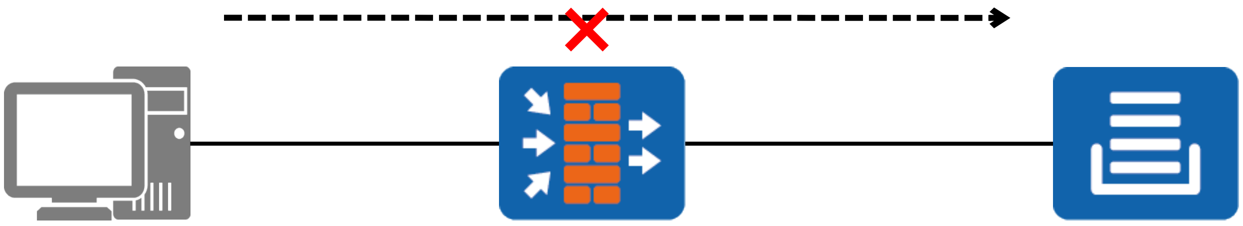
```
[NGFW]acl 2000
[NGFW-acl-basic-2000]rule permit source 20.0.0.1 0
```

- □□□□□□□□□□□□□

```
[NGFW]port-mapping FTP port 31 acl 2000
```

□□□□ © 2018 □□□□□□□□


20字节首部
0 0 0
...... 标识 0x1234 标志 片偏移 0 ...... 源IP地址 目的IP地址 选项 数据0+......+数据N
分片
0 0 1
第1片 ...... 标识 0x1234 标志 片偏移 0 ...... 源IP地址 目的IP地址 选项 数据0
0 0 0
第N片 ...... 标识 0x1234 标志 片偏移 N ...... 源IP地址 目的IP地址 选项 数据N



© 2018

□□□

1. □□□□□□□□□□□□□Server Map□□(   )

    A. □□NAT No-PAT

    B. □□NAT□□□□□

    C. □□ASPF

    D. □□□□□□□□□

2. □□□□□□□□□□□□4□□□□□□□□□□□□□□□□□□□□ □

    A. □□

    B. □□

[illegible]

- [illegible]
- [illegible]
- [illegible]

[illegible] © 2018 [illegible]

[illegible]

www.huawei.com